

## CLAIMS

1. Method for renewing a symmetric key in a communication network comprising a device of a first type (1) containing:

- 5                   - a first symmetric key ( $K_C$ ) for encrypting the data (CW) to be sent to a device of a second type connected to the network; and
- said first symmetric key ( $K_C$ ) encrypted ( $E2\{K_N\}(K_C)$ ) with a second symmetric network key ( $K_N$ ) known only by at least one device of a second type connected to said network.

10               the method comprising the steps that consist, for the device of a first type, in:

- (a) generating a random number (D);
- (b) computing a new symmetric key ( $K'_C$ ) as a function of the first symmetric key ( $K_C$ ) and said random number (D);
- 15           (c) encrypting the data to be transmitted (CW) with the new symmetric key ( $K'_C$ ); and
- (d) transmitting to a device of a second type (2), via said network:
  - the data encrypted with the new symmetric key ( $E3\{K'_C\}(CW)$ );
  - 20           - the random number (D); and
  - said first symmetric key encrypted with the second symmetric network key ( $E2\{K_N\}(K_C)$ ).

25               2. Method according to claim 1, wherein the function (f) used to compute the new symmetric key ( $K'_C$ ) is a one-way derivation function.

3. Method according to claim 2, wherein the function (f) is a hash or encryption function.

30               4. Method according to one of the previous claims, also comprising the steps consisting, for the device of a second type (2) that receives data transmitted at step (d), in:

- (e) decrypting, with the second symmetric network key ( $K_N$ ), the encryption ( $E2\{K_N\}(K_C)$ ) of the first symmetric key ( $K_C$ );
- 35           (f) determining, based on the first symmetric key ( $K_C$ ) obtained at step (e) and on said random number (D), the new symmetric key ( $K'_C$ ); and

(g) decrypting the data received with the new symmetric key ( $K'_C$ ) thus obtained.